

Fig. 1

101

Cipher Block Chaining Mode (CBC)

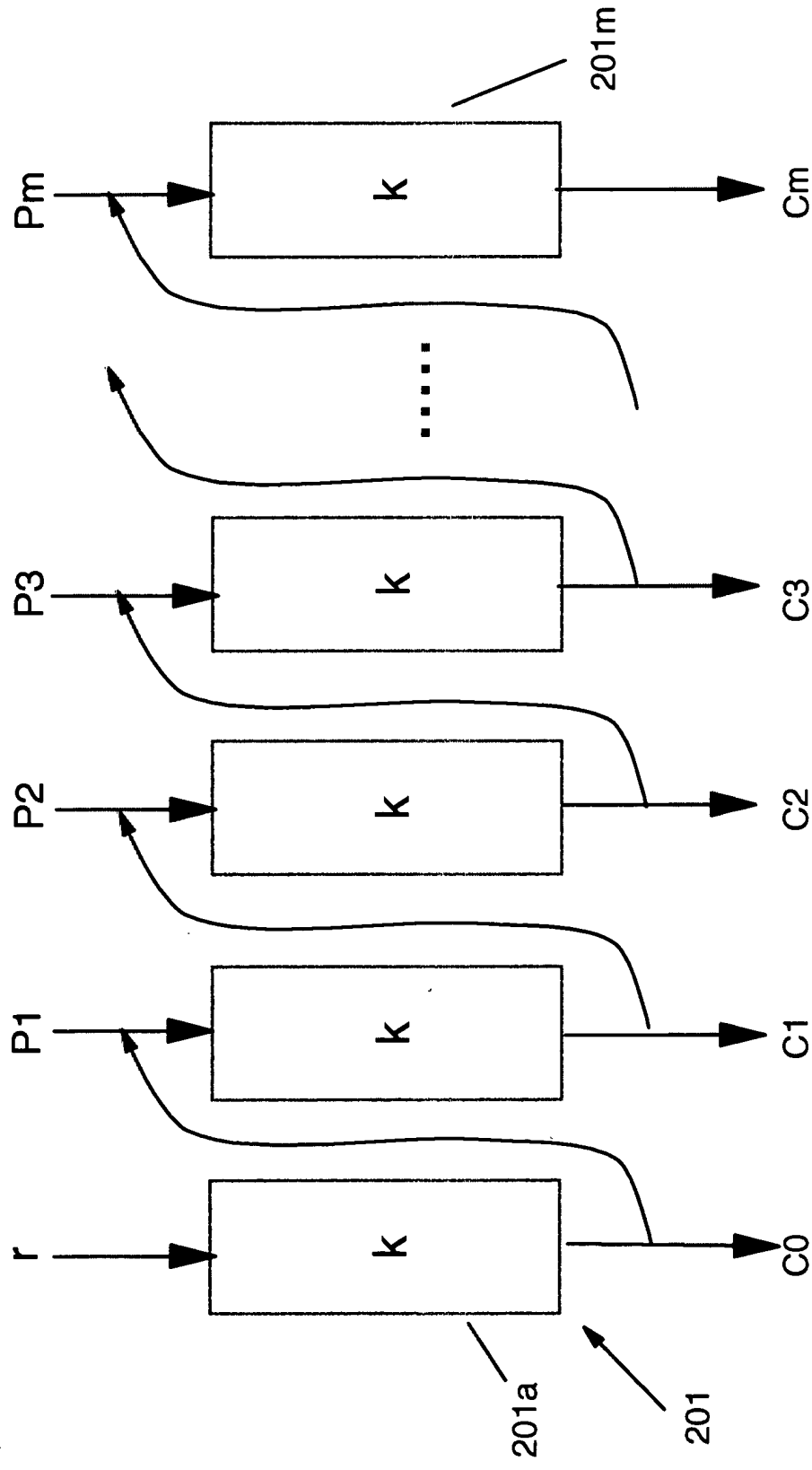


Fig. 2

103

CBC DECRYPT

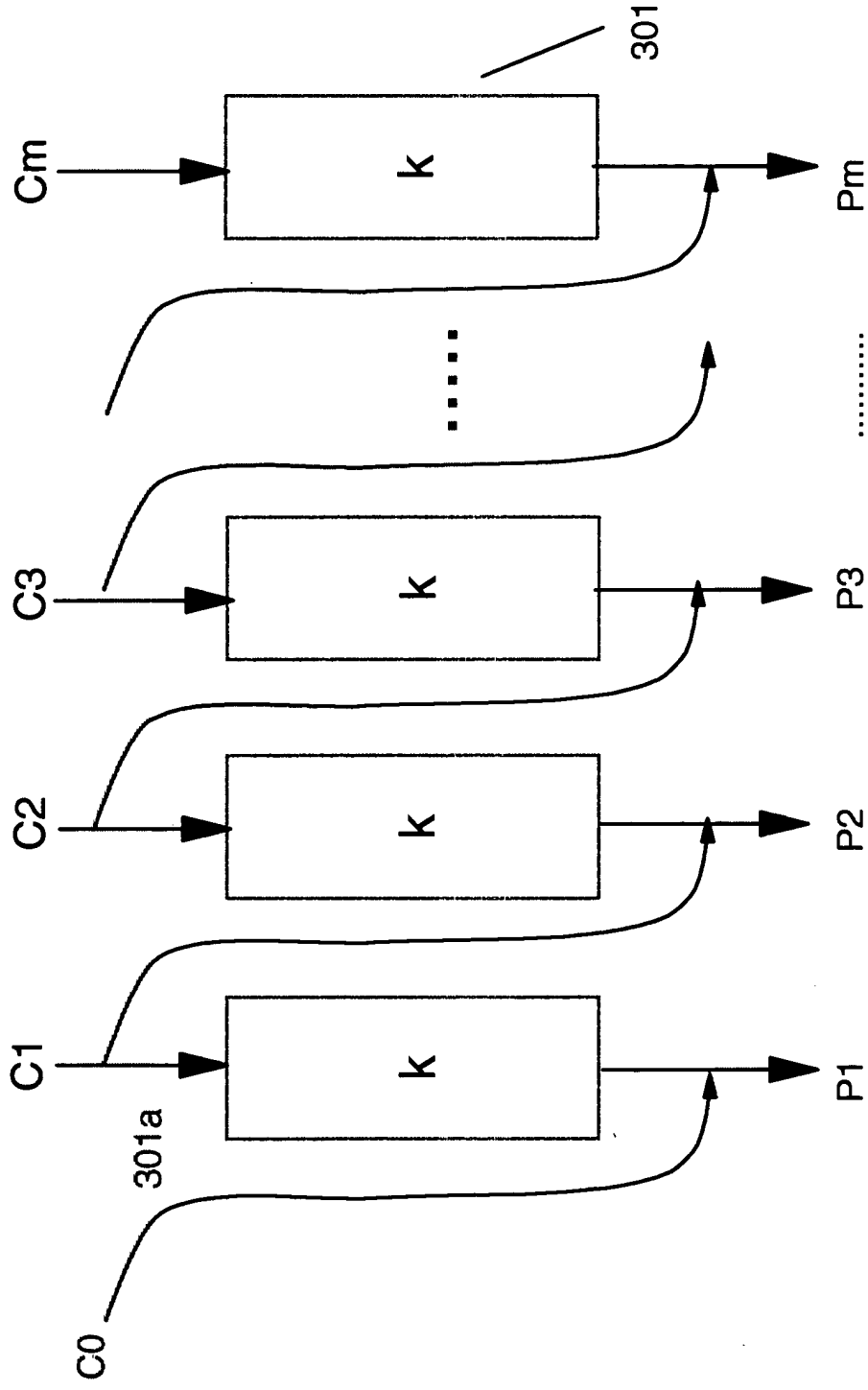


Fig. 3

400

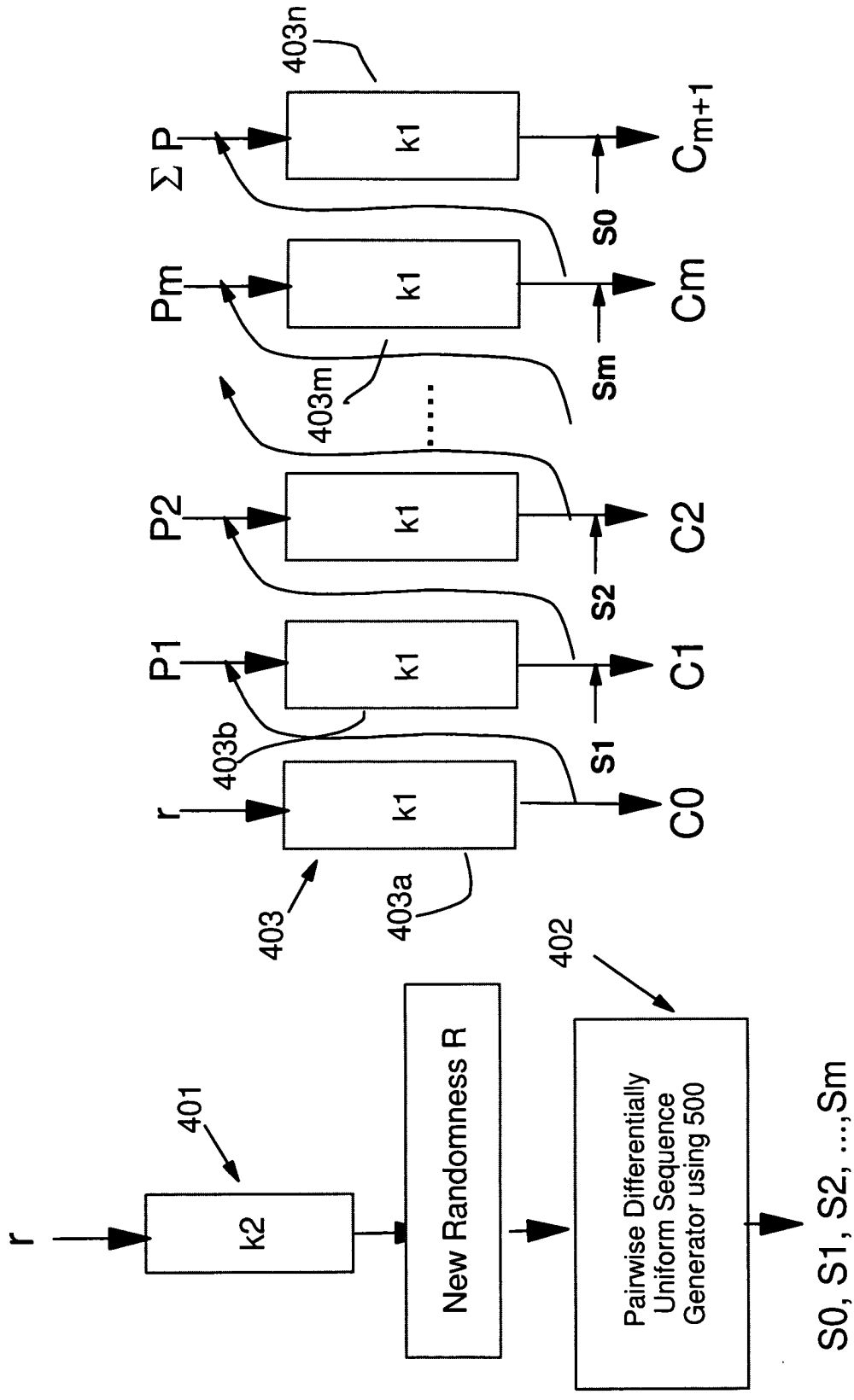


Fig 4

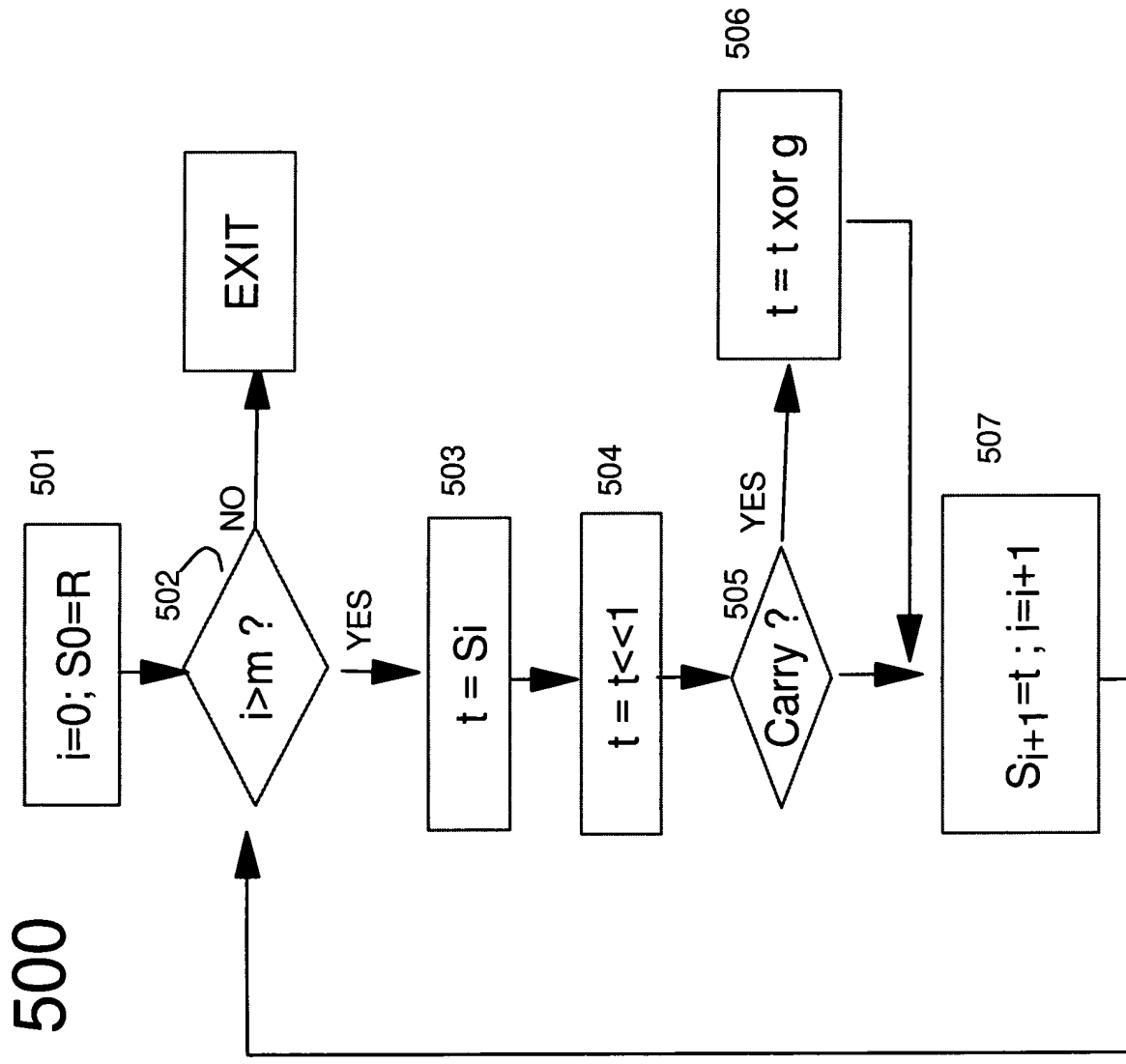


Fig 5

600

Ciphertext $C = \langle C_0, C_1, \dots, C_m \rangle$

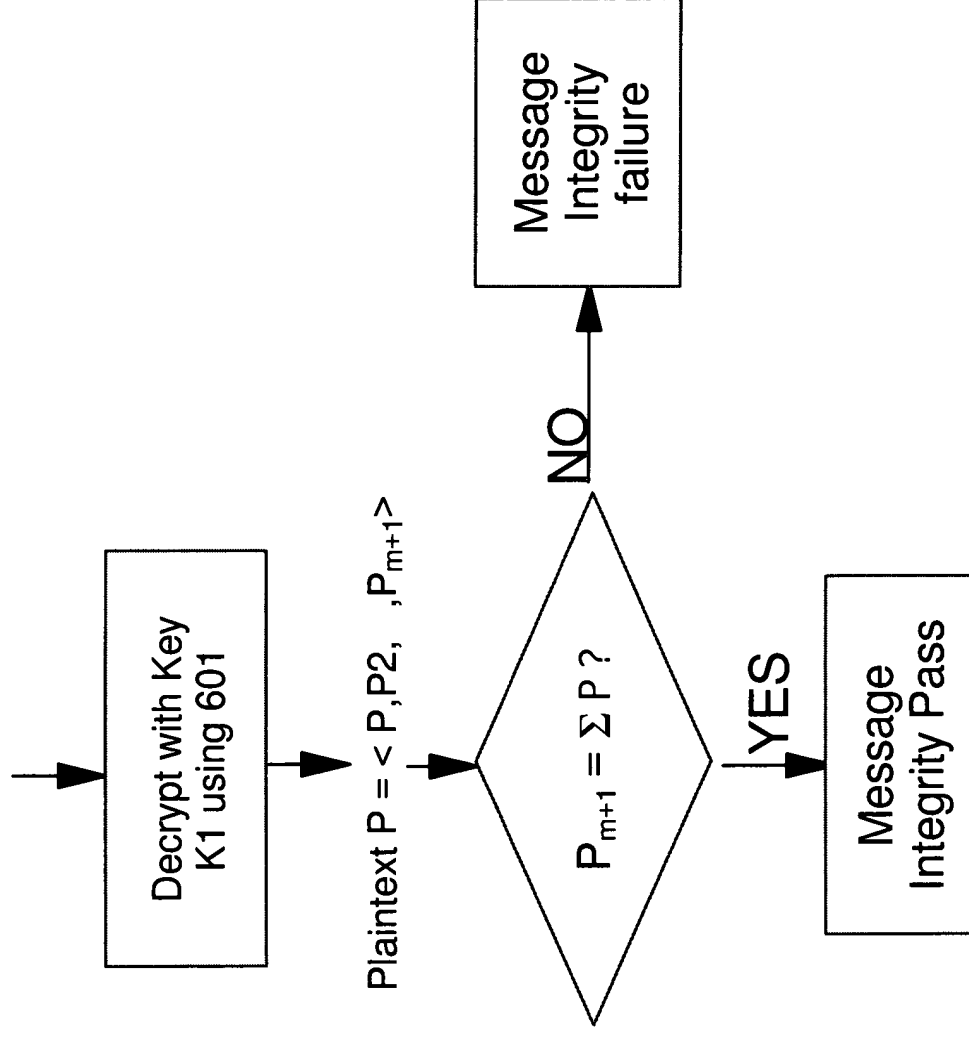


Figure 6

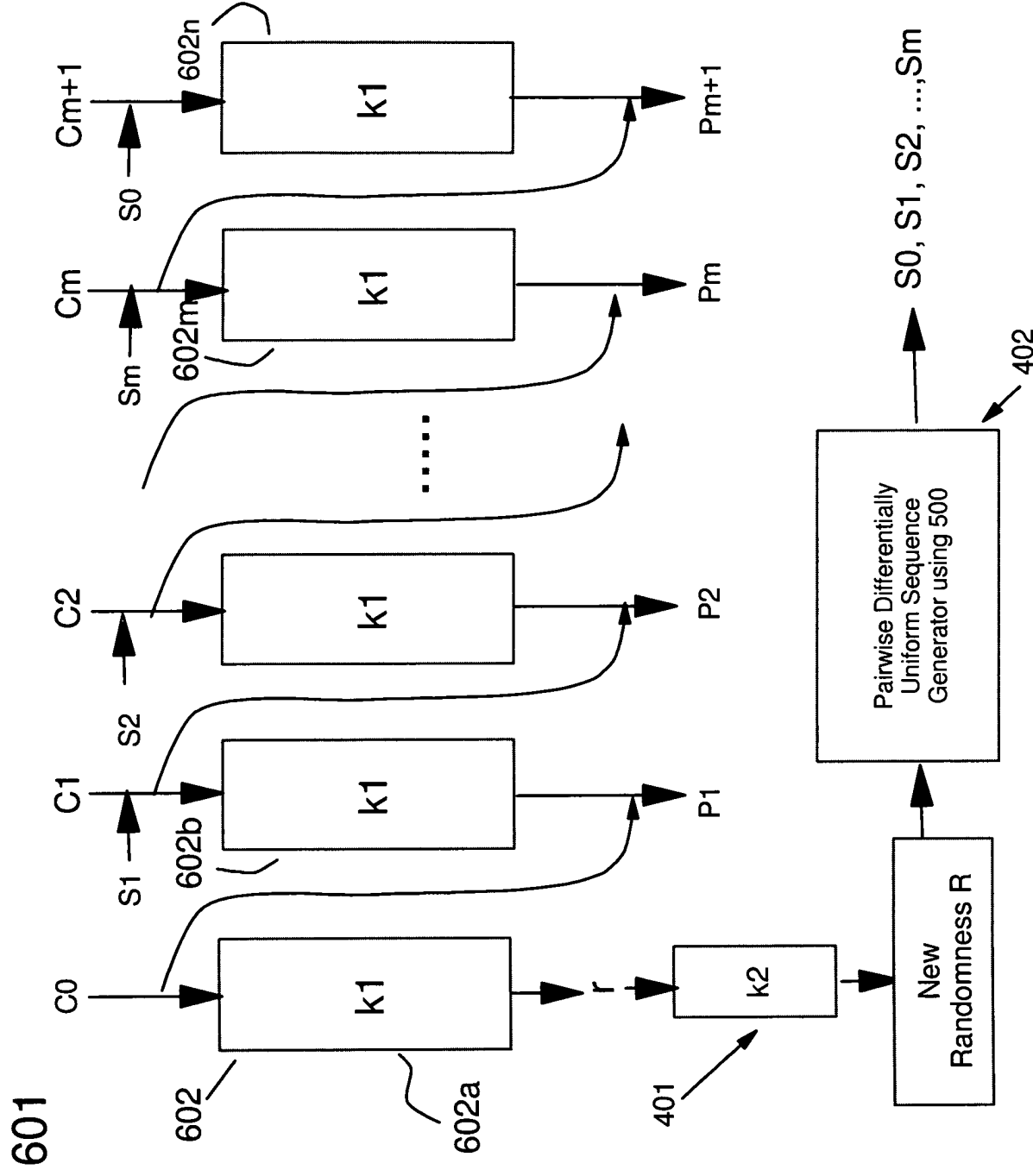


FIG 7

800

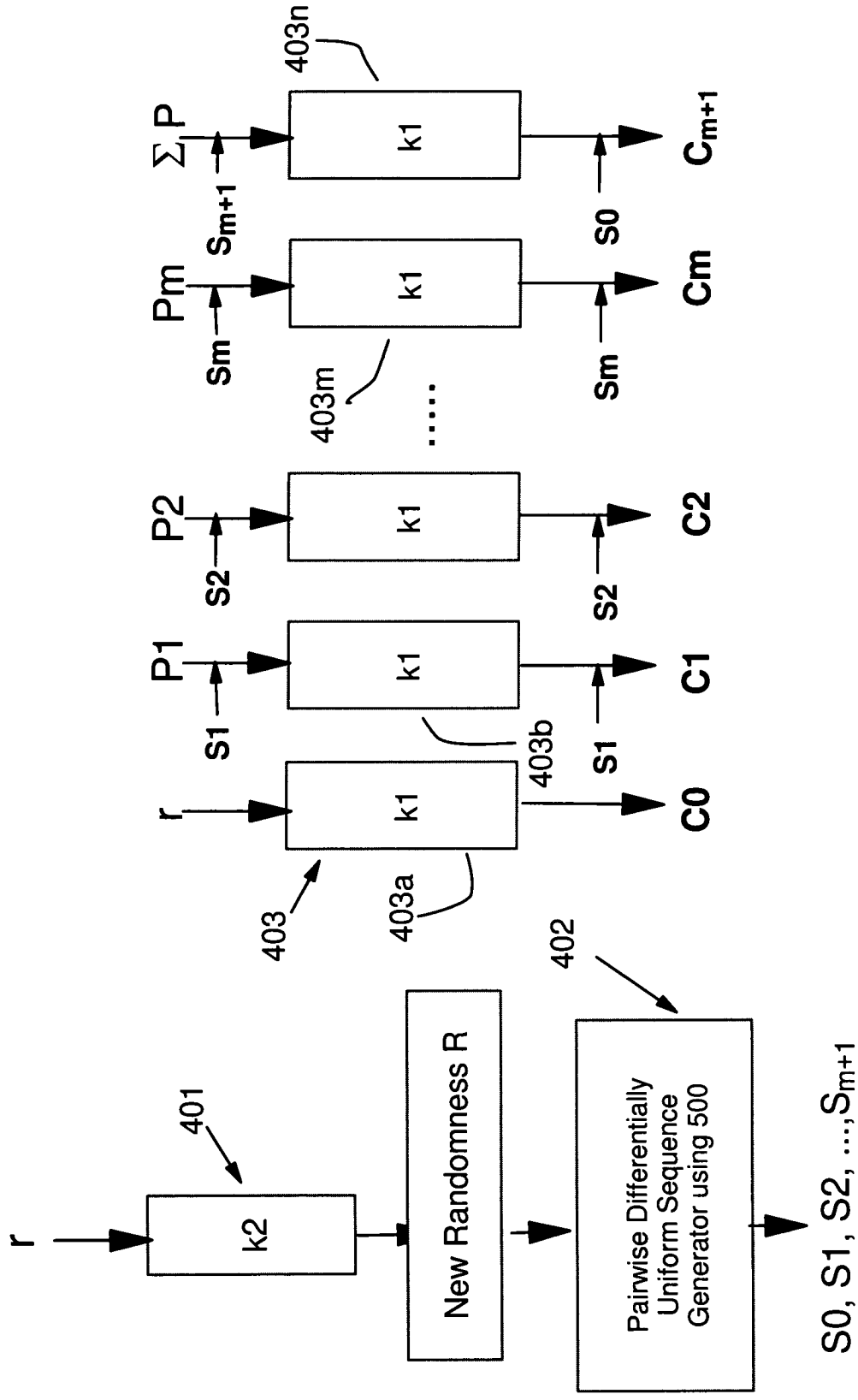


Fig 8

900

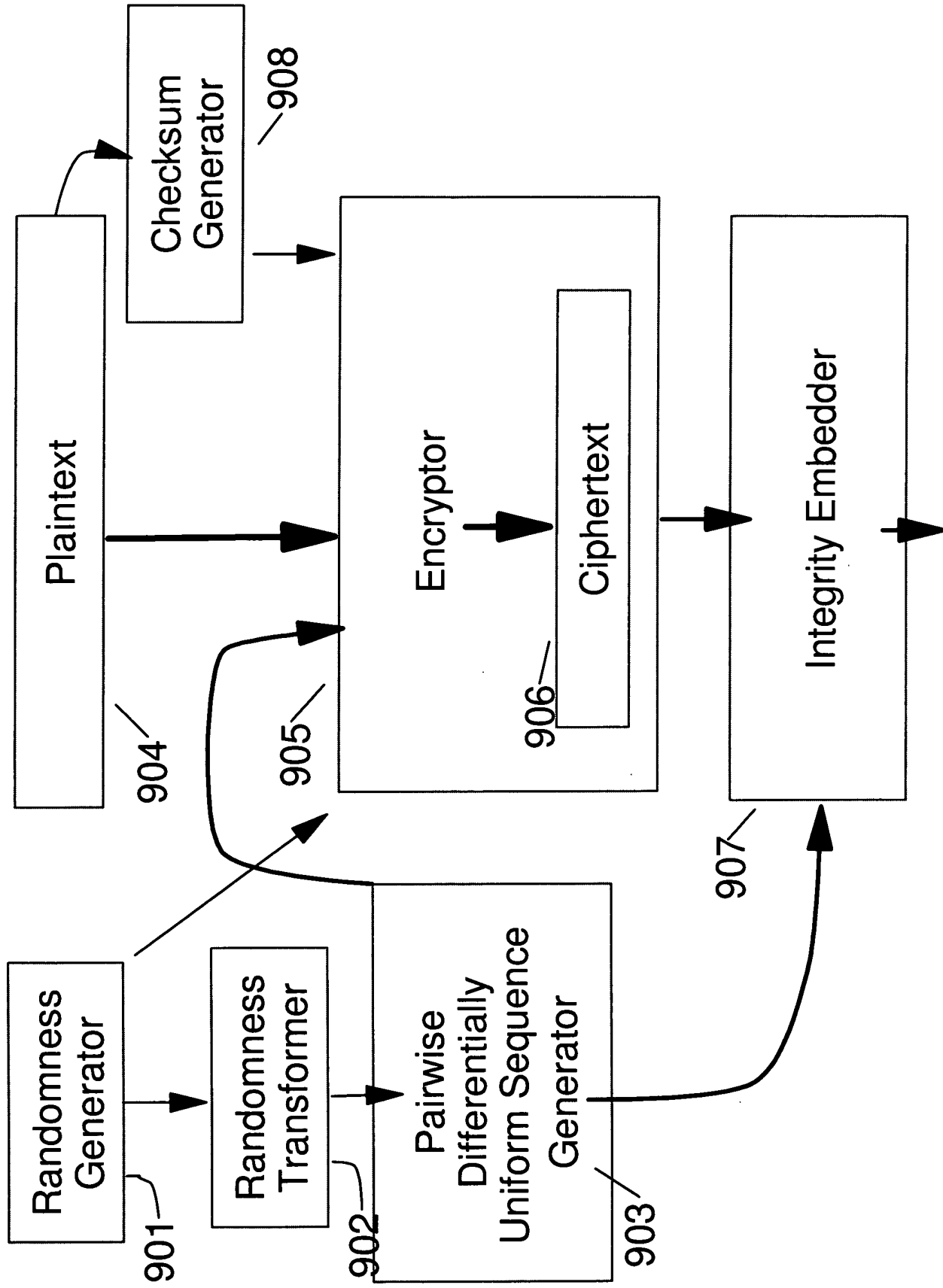


Fig 9

1000

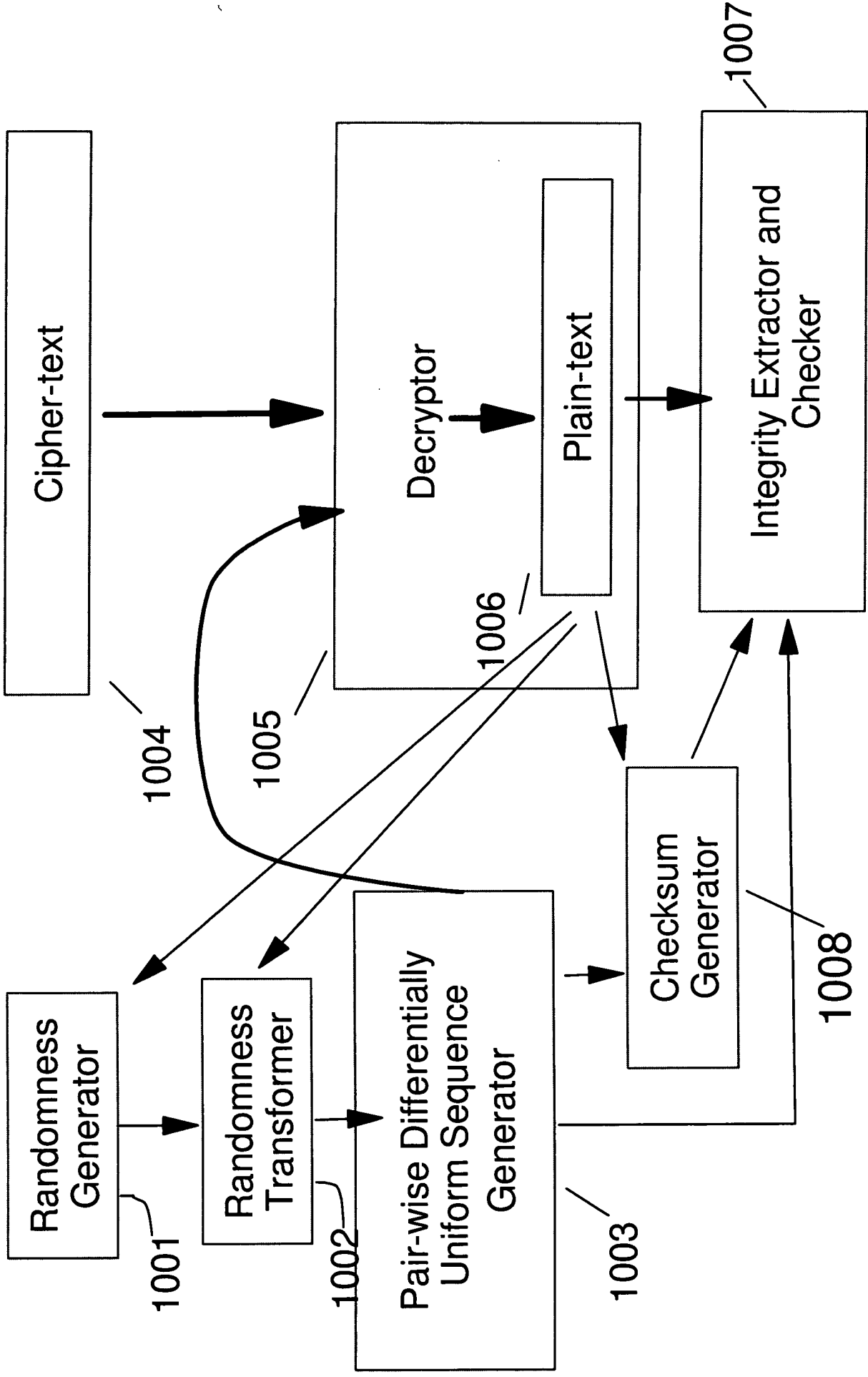


Fig 10

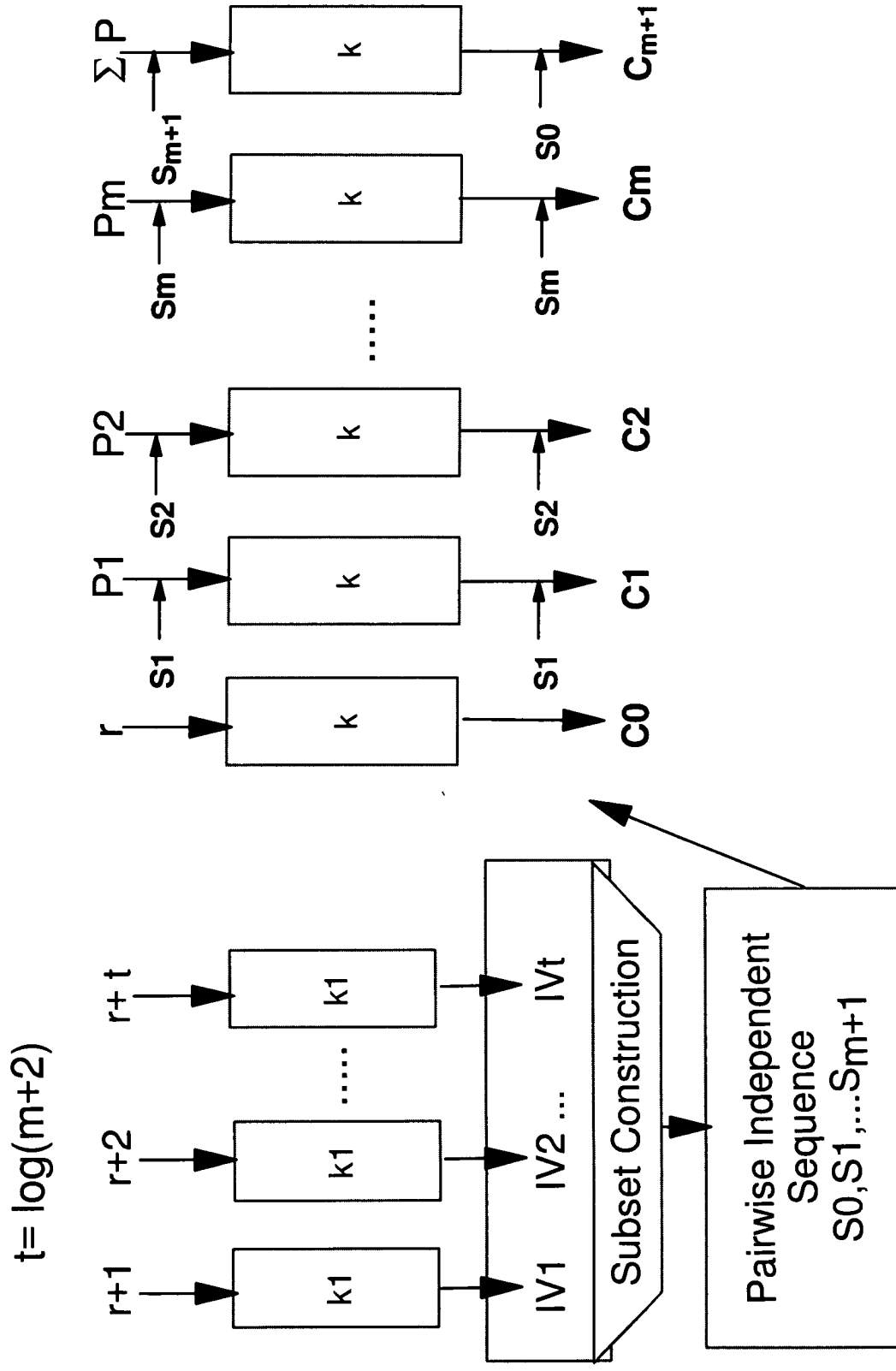


Fig 12